Insider Threat Study:

Illicit Cyber Activity in the Information Technology and Telecommunications Sector

Eileen Kowalski
National Threat Assessment Center
United States Secret Service
Washington, DC

Dawn Cappelli
Andrew Moore
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

January 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JAN 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**59**	

TABLE OF CONTENTS

SECTION 1: INTRODUCTION[1]

> *An employee of a company under contract to process health insurance claims defrauded his employers of millions of dollars by exploiting weaknesses in the design and implementation of the company's business processes. The employee, who was responsible for claims processing, took advantage of the lack of oversight or two-person control for checking claims entered into the system to enable individuals involved in organized crime external to the organization to construct and submit fraudulent claims to be approved by the company. The scheme diverted nearly $20 million from the company to the insider and his accomplices.*
>
> *An employee of a telecommunications firm's payroll department moved to a new position within the department in which she no longer would be required to have privileged access to payroll accounts. Upon switching positions, the employee's access rights to the payroll accounts were left unchanged. An associate told her that he was starting up a financial services business and needed some contact information. Using the privileged access rights that she had retained, the employee provided her associate with confidential information for 1500 of the firm's employees, including 401k account numbers, credit card account numbers, and social security numbers, which he then used to commit over 100 cases of identity theft. The insider's actions caused over $1 million in damage to the company and its employees.*
>
> *One night, an employee of a large telecommunications company embarked on a series of acts that he believed would enable him to "save the day" and impress his new supervisor. First, this employee used a contractor's badge to gain unauthorized physical access to the company's Network Operations Center (NOC), where all of the computers were left logged in with system administrator access. He then used those computers to bring down the system that provided address information for emergency 911 calls based on the incoming phone number for emergency services. Before leaving the NOC, he stole the backup tapes for the system. On his departure from the NOC, he proceeded to the backup offsite storage facility, where he gained unauthorized physical access to that facility by once again using the contractor's badge, and then stole additional system backup tapes. In all, 55 tapes were stolen. Fortunately, most areas affected by the employee's disabling of the central system were able to switch over to regional 911 systems; however, some areas had no 911 backup capabilities. These actions caused over $200,000 damage to the company.*

These incidents were all committed by "insiders" individuals who were, or previously had been, authorized to use the information systems that they eventually employed to

[1] Parts of this document reflect guidelines from the University of Chicago Press. The Chicago Manual of Style: The Essential Guide for Writers, Editors, and Publishers. 15th ed. The University of Chicago Press, Chicago.

perpetrate harm. Insiders have the potential to pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases.

The Insider Threat to Critical Infrastructures

The insider threat issue is a problem faced by all industries and sectors today. It is an issue of growing concern as the consequences of insider incidents can include not only financial losses, but the loss of clients and business days. The actions of a single insider can cause damage to an organization ranging from a few lost staff hours to negative publicity and financial damage so extensive that a business may be forced to lay off employees or even close its doors. Furthermore, insider incidents can have repercussions extending beyond the affected organization to include disruption of operations or services critical to a specific sector.

In *The National Strategy to Secure Cyberspace*[2], the President's Critical Infrastructure Protection Board emphasizes the importance of continual evaluation to identify vulnerabilities in, and threats to, government and private information networks and systems. In particular, *The National Strategy to Secure Cyberspace* stresses the need to maintain functioning networks and systems that are interconnected between thirteen critical infrastructure sectors[3] comprised of public and private institutions:

- Banking and Finance
- Information and Telecommunications
- Transportation
- Postal and Shipping
- Emergency Services
- Continuity of Government
- Public Health
- Food
- Energy
- Water
- Chemical Industry and Hazardous Materials
- Agriculture
- Defense Industrial Base

As most of America's critical infrastructure is privately held, a key component of the strategy is the strengthening of public-private partnerships to secure the collective infrastructure and improve national cyber security. The U.S. Department of Homeland Security is engaged in initiatives to enhance protection for critical infrastructure and

[2] The National Strategy to Secure Cyberspace. (February 2003). http://www.whitehouse.gov/pcipb/

[3] *Homeland Security Presidential Directive-7*, issued in December 2003, contains an updated description of the critical infrastructure sectors. Specifically, information technology and telecommunications are now designated as separate sectors. However, at the time this study was initiated the sectors were combined, and they are considered together for this report. See http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

networks by promoting working relationships between the government and private industry. One specific initiative promotes awareness of the insider threat to organizations.

The Efforts to Develop Information on the Insider Threat Issue

Efforts to identify prevalence of insider incidents

Estimates of how often government agencies and private companies are victimized by illicit cyber activity from within are difficult to make. It has been suggested that insider incidents are under-reported to law enforcement and prosecutors.[4] Reasons include insufficient damage to warrant prosecution, insufficient evidence to prosecute, and concerns about negative publicity should reports of the incidents surface.[5]

Moreover, statistics vary regarding the prevalence of incidents perpetrated by insiders compared to those perpetrated by individuals external to the target organizations.[6] The E-Crime Watch Survey™[7], carried out by the United States Secret Service (Secret Service), the CERT® Program of Carnegie Mellon University's Software Engineering Institute (CERT), and *CSO Magazine* in summer 2006, elicited responses from 434 security and law enforcement executives on issues related to electronic crimes. Fifty-five percent of the organizations that were victims of electronic crime reported one or more insider incidents or intrusions, with 58% of the incidents known or suspected to have come from outsiders, 27% from insiders, and 15% from unknown origin.

Efforts to address the insider threat issue

Previous efforts focused largely on groups that could be conveniently sampled or represented more narrow areas of industry. These initiatives included workshops to develop a foundation of knowledge on insider threats[8] and in-depth case studies of information technology (IT) insiders.[9] More recently, efforts aimed at addressing this issue have expanded to include

- annual surveys to identify the number of insider incidents experienced by organizations in a given year[10]

[4] National Research Council, Computer Science and Telecommunications Board, Summary of Discussions at a Planning Meeting on Cyber-Security and the Insider Threat to Classified Information, November 2000.

[5] CSO Magazine, United States Secret Service and CERT® Coordination Center. 2006 E-Crime Watch Survey. Framingham, MA: CXO Media [Hereafter referred to as 2006 E-Crime Watch Survey].

[6] Richardson, R. (2004). Ninth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute [Hereafter referred to as CSI Survey]; Deloitte Touche Tohmatsu (2005). 2005 Global Security Survey; 2005 E-Crime Watch Survey.

[7] http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

[8] Anderson, R. H. (1999, August). Research and Development Initiatives Focused on Prevention, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. Santa Monica, CA: RAND (CF151); Department of Defense (2000). DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team. Washington, DC.

[9] Shaw, E., Post, J., and Ruby, K. (August 31, 1999). Final Report: Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations.

[10] 2006 E-Crime Watch Survey; CSI Survey.

- workshops focused on mitigating the insider threat to the intelligence community[11]
- workshops to develop and test a framework for detection of insider activities that may pose threats to U.S. national security[12]

Individually, these initiatives have helped to expand the body of research and increase knowledge on this topic. However, gaps in the literature have made it difficult for organizations to develop a more comprehensive understanding of the insider threat. In particular, research to date has not examined the incidents from both behavioral and technical perspectives simultaneously. This lack of understanding has hampered efforts to address the issue from an approach that encompasses human resources, corporate security, and information security perspectives.

The Insider Threat Study (ITS) was initiated to take an in-depth look at reported insider incidents; specifically, the individuals who perpetrate these incidents and the types of incidents that have occurred within critical infrastructure sectors from both a behavioral and technical perspective. It is a collaborative initiative of the Secret Service National Threat Assessment Center (NTAC) and the CERT® Program of Carnegie Mellon University's Software Engineering Institute (CERT). The ITS was funded in part by the Department of Homeland Security, Office of Science and Technology.

[11] Anderson, R. and Brackney, R. (2004). Understanding the Insider Threat: Proceedings of a March 2004 Workshop. http://www.rand.org/publications/CF/CF196/

[12] http://www.mitre.org/news/events/tech04/8.html

The Secret Service/CERT Collaboration

Since 2001, the Secret Service and CERT have collaborated in an array of efforts to identify, assess, and manage potential threats to, and vulnerabilities of, data and critical systems. This collaboration represents an effort to augment security and protective practices by

- finding ways to identify, assess, and mitigate cyber security threats to data and critical systems that impact physical security or threaten the mission of the organization
- finding ways to identify, assess, and manage individuals who may pose a threat to those data or critical systems
- developing information and tools that can help private industry, government, and law enforcement identify cyber security issues that affect physical or operational security and assess potential threats to, and vulnerabilities in, data and critical systems

The Insider Threat Study (ITS) is a central component of this Secret Service/CERT multi-year collaboration. The ITS focuses in particular on the *people* who use or exceed their authorized access to information systems to perpetrate harm to organizations. The prevention of insider activity is important to the Secret Service because it can adversely affect the investigative and protective missions of the agency. Specifically, the Secret Service investigates:

- violations of law related to financial crimes that include, but are not limited to, financial institution fraud, identity theft, access device fraud, and computer fraud
- computer-based attacks on our nation's financial, banking, and telecommunications infrastructure
- cyber security incidents, such as acts of sabotage, that cause the failure or compromise of information systems critical to the protective mission

The project draws from the Secret Service's expertise in behavioral and incident analysis and CERT's technical expertise in network systems survivability and security. Previous Secret Service studies have focused on identifying the thinking and behavior of subjects known to have posed a threat to public officials, public figures,[13] and school children.[14] Information developed from these studies has proven to be operationally relevant in preventing future violent or disruptive incidents. The goal of this earlier research was to gather information to enhance threat assessment efforts – efforts to identify, assess, and manage the risk of harm an individual may pose before that individual has an opportunity to engage in violent, or disruptive, behavior.

[13] Fein, R. A., and Vossekuil, B. (January 2000). Protective Intelligence & Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials. U.S. Department of Justice.

[14] Vossekuil, B., Fein, R., Reddy, M., Borum, R., and Modzeleski, W. (June 2004). The Final Report and Findings of the Safe School Initiative: Implications For The Prevention of School Attacks in the United States. United States Secret Service and United States Department of Education.

Previous CERT research, sponsored by the U. S. Department of Defense (DoD), focused on cyber insider threats in the military services and defense agencies. That work effort is part of an ongoing partnership between CERT and the Defense Personnel Security Research Center (PERSEREC) undertaken in response to recommendations in the 2000 *DoD Insider Threat Mitigation* report.[15] The focus of that partnership is to identify characteristics of the environment surrounding insider cyber events evaluated for criminal prosecution by DoD investigative services. The primary use of this information will be to guide future operating, security, and personnel procedures to reduce the threat to critical information systems in the DoD and its contractor community. Since then, the CERT/PERSEREC partnership has been expanded to explore whether it is possible to develop predictive models of adverse insider behavior that consider technical deterrents as well as social, organizational, and psychological factors; and whether these models may apply to espionage as well as IT insider sabotage, both examples of trust betrayal.[16]

The Insider Threat Study

Initiated in 2002, the Insider Threat Study is a multi-year exploration of employees who have perpetrated acts of harm against an organization via computer system or network to include theft of intellectual property, fraud, and acts of sabotage within critical infrastructure sectors. The overall objective of the ITS is to help private industry, government, and law enforcement better understand, detect and possibly prevent harmful insider activity. A particular focus of the study is to identify information that may have been discernable prior to the incident from both a behavioral and technical perspective.

The ITS consists of the following components:

- an annual survey, conducted over a three-year period, to estimate the prevalence of insider activity experienced by a sample of public and private sector organizations[17]
- several in-depth case study analyses of insider incidents that occurred within the banking and finance, information technology and telecommunications (IT), and government critical infrastructure sectors
- an aggregate analysis of insider incidents across the critical infrastructure sectors where sabotage was the goal or intent

Reports from this study are written for a diverse audience that includes

- business executives
- human resources personnel
- technical professionals

[15] www.defenselink.mil/c3i/org/sio/iptreport4_26dbl.doc

[16] Band, S.R., Cappelli, D.M., Fischer, L.F., Moore, A.P., Shaw, E.D., Trzeciak, R.F. (2006, December). Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Report available at http://www.cert.org/archive/pdf/06tr026.pdf

[17] CSO Magazine, United States Secret Service and CERT® Coordination Center. (2006). 2005 & 2004 E-Crime Watch Survey. Framingham, MA: CXO Media.

- security professionals
- law enforcement professionals
- legislators
- prosecutors

The study has resulted in a series of four case study reports. The first report, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* published in August 2004,[18] examined 23 incidents of insider threat in the banking and finance sector. The second report*, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,*[19] published in May 2005, examined 49 insider incidents across critical infrastructure sectors in which the insider's primary goal was to sabotage some aspect of the organization (for example, business operations, information/data files, system/network, and/or reputation) or direct specific harm toward an individual.

This report, *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*, presents the third series of findings on 52 incidents from this multi-year research effort in which the target organizations were in the Information Technology and Telecommunications Sector. The fourth report in the series, *Insider Threat Study: Illicit Cyber Activity in the Government Sector*, examines 36 incidents of illicit cyber insider activity that fall within the government sector.

Study Purpose

The Insider Threat Study research effort was undertaken to: 1) identify any pre-incident communications or behaviors exhibited by employees to include physical, social, and on-line behaviors; 2) identify vulnerabilities exploited by employees to carry out their illicit activities; and, 3) examine insider activity as it relates to critical infrastructure sectors.

Researchers examined insider activity within the critical infrastructure sectors for two primary reasons. Mainly, insider activity within the banking and finance, IT, and government sectors directly affects cases investigated by the Secret Service. Additionally, at the start of this study, a comprehensive examination of insider activity within or across these sectors had not been conducted despite the fact that protecting the critical infrastructures was, and is, considered a national priority.

Research Questions

Several fundamental questions guided the ITS research:

1. Are there pre-incident behavioral or technical activities, plans and communications that can be identified to inform how or why a person moves from the idea of targeting to the actual act of harm?

[18] Available on-line at http://www.cert.org/archive/pdf/bankfin040820.pdf and http://www.secretservice.gov/ntac/its_report_040820.pdf

[19] Available on-line at http://www.cert.org/archive/pdf/insidercross051105.pdf and http://www.secretservice.gov/ntac/its_report_050516.pdf

2. Are there investigative and protective implications of insider activity for the Secret Service?
3. What is the nature and impact of insider activity to specific critical infrastructure sectors?
4. Were there key life events or patterns in the histories of people who have targeted organizations for harm?
5. What are the technical details of how the insider conducted the incident?

Methodology

Study Definition

The cases examined in the ITS are incidents perpetrated by insiders. Insiders are defined as current, former, or contract employees who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations. Only those cases meeting the study definition(s) that occurred in the United States between 1996 and 2002, in an organization that fell within a critical infrastructure sector, were included in this study.

Study Sample

A total of 149 cases across 12 of the 13 critical infrastructure sectors were identified through public reporting and searches of Secret Service case files. Public reporting included references in various media outlets, found through searches on Lexis-Nexis news and court databases and Internet searches.

Research and Analysis

For each case examined in the study, researchers from the Secret Service and from CERT traced the insider incidents backwards in time from the initial point of harm to when the idea of committing the incident first occurred to the insider. In retracing these incidents to their origins, researchers identified insider behaviors, communications, and activities – both online and offline – prior to and during execution of the incidents.

Researchers also reviewed primary source materials, as available and applicable, that included police reports, federal law enforcement investigative reports, court records, mental health records, arrest records, accounts by third parties of the insider's history and behaviors, and secondary source material from news articles. Information gathered for each case included descriptive, demographic, behavioral, and historical data about each insider and facts about the insider's work history within the affected organization. Information gathered on the organization included demographic data; descriptions of the organization's policies and technical security measures and specific damage suffered by the organization. Technical information gathered included details of how the incident was planned and carried out; and technical activity to set up the incident.

This type of social and environmental information was not always included in the source materials collected. For that reason, ITS researchers conducted supplemental interviews, when possible, in an attempt to obtain information beyond these materials.

Researchers attempted to conduct at least one supplemental interview per case. Interviews were conducted with case investigators, organization representatives, prosecutors and a few insiders themselves.[20]

Researchers used the information gleaned from these sources to answer several hundred questions about the insider and the behavioral and technical aspects of the incident.[21] The questions were organized around the following major topic areas:

- components of the incident
- detection of the incident and identification of the insider
- pre-incident planning and communication
- nature of harm to the organization
- law enforcement and organizational response
- characteristics of the insider and the organization
- insider background and history
- insider technical expertise and interests

Specific examples of behavioral areas of inquiry included

- whether the insider had a plan to commit the harm
- the insider's motive for committing the incident
- whether the insider communicated any prior interest in harming the organization
- whether the insider displayed any concerning or noticeable behaviors prior to the incident
- whether the insider had a record of disciplinary actions at work
- whether the insider faced legal consequences

Specific examples of technical areas of inquiry included

- the insider's level of access at the time of the incident
- technical methods and tools used
- whether an account was compromised
- whether remote access was used
- which system logs were utilized to identify the insider
- the insider's level of experience with and interest in computers, hacking, programming, etc.

Questions pertaining specifically to the target organization included descriptive information on the organizations' methods of operations, structures, areas of business; and questions pertaining to policies regarding termination, acceptable use, and system back-ups.

Despite ITS researchers' best efforts, sources did not yield information to answer every question for all cases. For this reason, percentages in this report are based on the total number of cases for which information was available for a given research question. For

[20] For this report, researchers interviewed representatives from at least 9 companies and at least 20 law enforcement or prosecutorial agencies.

[21] Information from the insider interviews was used to answer questions when corroborated.

example, if information for a particular research question was available for only 26 of 36 incidents, then 26 is 100% for that particular question.

In addition, some research questions in this study concern the insider, while others bear on the incident. Accordingly, the denominator will vary depending upon whether the finding pertains to the insider or the incident itself. Instances in which information for a particular research question was not available for more than 10% of the cases are indicated by a footnote.

Limitations

As noted previously, private and public organizations may be reluctant to report incidents of illicit cyber activity, even to law enforcement, suggesting that the actual number of insider cases may be significantly greater than those to which the research team had access. Suspected underreporting of insider incidents also makes it difficult to assess what percentage of all cases are represented in the ITS. Accordingly, this report and others from the study will present only what was found among the known cases. This limits the ability to generalize the study findings from cases examined to the unknown universe of all incidents or experiences in a given sector and underscores the difficulty other researchers have faced in trying to better understand the insider threat.

Nevertheless, limitations associated with the number of cases examined by the ITS do not diminish the value of the knowledge that can be gained from analyzing these incidents. The study findings provide insight into actual criminal and other illicit acts committed by insiders. This insight may be useful to those individuals in the sectors charged with protecting critical assets as they begin to examine ways of improving their defense against insider threats.

Overview of Findings in the IT Sector

This ITS report examines 52 incidents carried out by 57 insiders that occurred in the information technology and telecommunications sector (IT) between 1996 and 2002.[22] Of the 52 incidents, 24 involved solely sabotage; 11 involved solely theft of intellectual property; 8 involved solely fraud; 6 involved both sabotage and theft of intellectual property; and 3 involved both fraud and theft of intellectual property.

Organizations affected by insider activity in this sector included

- internet service providers
- companies conducting e-business
- software, hardware, network, and telecommunication equipment manufacturers and suppliers
- newspapers
- companies that provide information technology and telecommunications-related technical consulting services

[22] Eight percent (4/52) of the cases involved multiple subjects.

The key findings of this report include

- current and former employees carried out insider activities.
- most insiders held technical positions within the target organization.
- most insiders' actions were triggered by a specific work-related event.
- the majority of insiders planned their activities in advance.
- some insiders had prior arrests.
- half of the insiders had authorized access to the system/network at the time of the incidents.
- over half of the insiders used relatively sophisticated tools or methods for their illicit activities, including scripts or programs, autonomous agents, toolkits, probing, scanning, flooding, spoofing, compromising computer accounts, or creating unauthorized backdoor accounts.[23]
- insiders committed their illicit activities both from within the workplace and remotely.
- the incidents took place during and outside normal working hours.
- most of the insider incidents were only discovered through manual (non-automated) detection of an irregularity or failure of an information system.
- the majority of insiders took steps to conceal their identities and their activities.

Organization of the Report

The remainder of this report is organized into the following sections. Section 2 presents the key findings of the study. Section 3 discusses the key findings and their implications for the development of prevention strategies. Section 4 offers some concluding thoughts.

Additionally, this report includes five appendices. Appendix A provides tables containing information on the date of the incidents and headquarters locations of the affected organizations examined by this study. Appendix B provides tables on the size of the target organizations and the amount of financial damage to these organizations. Appendix C contains additional case examples examined for this study. Appendix D contains a glossary of technical terms used in this report. The first use of each term included in the glossary is underlined in the text of the report. Appendix E identifies and acknowledges the efforts of individuals who worked on this project.

[23] Appendix D contains a glossary of technical terms used in this report. The first use of each term included in the glossary is underlined in the text of this report.

Section 2: Key Findings of the Insider Threat Study of Illicit Cyber Activity in the IT Sector

The key findings of the study of illicit incidents of insider activity within the information technology and telecommunications sector are presented under four categories:

- The Insiders
- The Target Organizations
- The Attacks
- The Consequences of the Attacks

The first section, *The Insiders*, is comprised of two subsections, the first of which presents key findings related to characteristics of the individuals who perpetrated the attacks examined for this study; the second presents findings concerning the insiders' motives and goals for the attacks.

The second section, *The Target Organizations*, presents key findings concerning the types of organizations targeted, their sizes, their locations, and the number of incidents occurring during the period examined by the ITS.

The third section, *The Attacks*, reports key findings related to the insiders' pre-attack behaviors and planning; the means by which the attacks were carried out; and the manner in which the attacks were detected and the insiders identified.

The fourth section, *The Consequences of the Attacks*, is comprised of two subsections. The first of these subsections reports on key findings related to the insiders' perceptions of the potential consequences of their actions; charges brought against insiders following investigation of the attacks; and the disposition of cases prosecuted against insiders. The second subsection reports on key findings related to the harm inflicted by the insiders on the target organizations.

The Insiders

Characteristics

Key Findings

- Current and former employees carried out illicit insider activities in nearly equal numbers.
- Most insiders were either previously or currently employed full-time in a technical position within the organization.[24]
- Thirty-eight percent of the insiders had been arrested previously.[25]
- Insiders represented a wide range of ages, from 17 to 58 years.[26]

[24] A technical position is one requiring specialized skills in information and technology, including programming, scripting, networking, information security, or system architecture and configuration.

[25] Data were only available for 47 of the 57 insiders studied.

- Insiders represented a variety of racial and ethnic backgrounds.
- The majority of insiders were single at the time of the attack, and had never been married.
- Insiders were predominantly male.

Supporting Data
At the time of the incident, 53% of the insiders were current employees or contractors of the affected organizations and 47% were former employees or contractors.

The former employees or contractors left their positions for a variety of reasons, to include resignation (41%), being fired (37%), being laid off (7%), expiration of their employment contracts (7%), and other reasons (8%).

Most of the insiders (76%) were full-time employees of the affected organizations, either before or during the incidents. Eighteen percent had been hired as contractors or consultants, 4% of the insiders worked as temporary employees, and 2% worked part-time.

Sixty-three percent of the insiders were employed in technical positions, including engineers (25%); system administrators (22%); programmers (22%); information technology specialists (14%); and other technical positions (14%). Eighteen percent were employed in a professional position such as sales specialist, account manager, editor, or analyst. Of the remaining insiders, 7% were employed in executive management or supervisory management positions; 7% worked in customer service positions; and 5% held administrative/clerical support positions.

Although the majority of insiders (62%) did not have a prior arrest history, 38% of the insiders had been arrested for a criminal act prior to carrying out the attack.[27] Of those insiders, offenses included: larceny and aggravated assault (39%), financial/fraud related offenses (33%), and alcohol or drug related offenses (28%). Over half (56%) of those insiders with a prior criminal history had multiple prior arrests and convictions.

The insiders' demographics varied. Insiders ranged in age from 17 to 58 years.[28] Ninety-one percent of the insiders were male, a finding that arguably reflects national statistics indicating technical occupations are traditionally male-dominated in the U.S.[29] Fifty-seven percent of the insiders were single at the time of the incident, while 35% were married, and 6% were divorced.

[26] Data were only available for 48 of the 57 insiders studied.

[27] Data were only available for 47 of the 57 insiders studied.

[28] Data were only available for 48 of the 57 insiders studied.

[29] According to the U.S. Department of Labor Bureau of Labor Statistics, in 2004 73% of all employees in Computer and Mathematical occupations were male. http://www.bls.gov/cps/cpsaat9.pdf

Motives

> *Denied a request for a raise and transfer to a company location closer to his home, one insider angrily resigned from his position. While the company required most employees who resigned to leave the premises immediately following their resignations, this insider, by virtue of his positive relationship with the owner of the company, was allowed to keep working in his position for an additional two weeks.*
>
> *During this two week time frame, the employee planned and executed the theft of company proprietary information. His goal in taking this information was to use it as reference material to improve his chances of gaining new employment. The insider transferred the information to an open storage area on a company server, then went home and used a popular file transfer method to download it to his home computer. His supervisor noticed the file transfer in progress, interrupted the transfer, and notified police.*

Key Findings

- A specific event or series of events triggered most insiders' actions.
- Multiple motives were reported for the majority of insiders. Revenge was reported as the main motive in just over half the cases.
- The most frequently reported goals of insider attacks were financial gain, theft of information/property, and sabotage to the organization.

Supporting Data

In 73% of the cases, a specific event or a series of events triggered the insiders' actions.

- Sixty-seven percent of the cases involved work-related events, including employment termination (37%); disputes with a current or former employer (20%); employment-related demotion or transfer (5%); and employment-related discipline (5%).
- Thirty-three percent of the incidents were initiated for reasons unrelated to the subjects' employment within the affected organizations, including employment with a new company (12%); individuals unrelated to the organization that spurred the insider to carry out the activities (12%); and other personal reasons (9%).

Fifty-six percent of all insiders were motivated at least in part by a desire to seek revenge.[30] Insiders were also motivated to commit their attacks to

- achieve financial gain (37%)
- redress a grievance or an issue of concern to the insider (30%)
- address dissatisfaction with company policies (12%)
- take information with them to their new employers (11%)

[30] Multiple responses possible; total may be over 100%.

Fifty-three percent of the insiders had multiple motives for carrying out their actions. Forty-seven percent of insiders had a single motive.

Forty-seven percent of the insiders had multiple goals.[31] Insiders' primary goals were to[32]

- sabotage the organizations' data, systems, or networks, business operations, or reputations (47%)
- achieve financial gain and/or steal information/property (42%)
- inflict harm on specific individuals (4%)
- maintain/gain leverage in their positions within the target organizations (4%)
- achieve some other goal (4%)

Fifty-six percent of the insiders held a grievance prior to the incident, and in 93% of these cases the insiders' grievances were work-related (including grievances against current and/or former employers, supervisors, and coworkers). Thirty-two percent of the insiders were perceived by others as disgruntled employees.[33]

The Target Organizations

Key Finding

- The majority of the target organizations employed 500 or fewer individuals.

Supporting Data

Sixty-two percent of the organizations targeted in incidents examined for this sector employed 500 or fewer individuals, while 30% had at least 10,000 employees. Appendix B provides a table on the affected organizations' sizes by numbers of employees.

Twenty-nine percent of the organizations targeted were headquartered in California. Five states – Washington, Florida, New York, New Jersey, and Pennsylvania – were headquarters to three organizations each. Appendix A provides a table on the location of the affected organizations' headquarters.

All of the affected information technology and telecommunications companies who were the targets of attacks examined by the ITS were in private industry. Fifty percent of the affected organizations conducted business domestically only while 50% conducted business both domestically and internationally.

[31] For each insider, researchers coded both the insider's motive (the reason or reasons why the insider engaged in the incident; for example, revenge) and the insider's goal (what the insider was trying to accomplish with the incident; for example, destroying the company's reputation).

[32] Multiple responses possible; total may be over 100%.

[33] By way of example, almost 1/3 of the technical insiders who carried out attacks examined in this report were found to have made attempts to move up in the technical hierarchy (31%) within their respective organizations. Among those insiders, just under half (45%) were not successful in doing so.

The frequency of incidents varied slightly between 1996 and 2002. The highest number of incidents reported for a single year occurred in 1998 (20%). The lowest number of incidents were reported in 1997 and 2002 (10% each respectively). The number of incidents reported each year gradually declined from 1998 to 2002. Appendix A provides a table on the number of incidents by year.

Of the twenty cases involving "theft of intellectual property," almost half of these insiders were requested to sign a non-disclosure agreement or were aware of policies regarding confidentiality.

The Attacks

Pre-attack Behaviors and Planning

> *The insider, a sales representative, had his compensation steadily decreased due in part to his being a "chronically unhappy employee." Upset by his deteriorating status within the company, the insider told a colleague that if he left the organization, he would take all of his business accounts and 20% of the company's other accounts with him. When the insider in fact accepted an offer for employment with a new company, he falsely informed his supervisor that he had received an offer, but had turned the position down. Over a month's time, while waiting for the new job to start, the insider forwarded more than 100 confidential email messages to his home computer. Several of these messages contained passwords for accessing secure areas of his employer's network and proprietary information on a computer program that the insider had helped build (and he was of the opinion he rightfully owned). The passwords allowed the insider to view confidential customer information to which he did not have access during his normal course of duties. His goal was to take this information to his new employer. The insider deleted the contents of his hard drive to cover his tracks, and then submitted his resignation.*

Key Findings

- The majority of insiders planned their activities in advance.
- The majority of insiders came to the attention of someone in the workplace for problematic or unusual behavior prior to the incident.
- Others had information about the insiders' intentions, plans, and/or ongoing activities.

Supporting Data

Seventy-six percent of the insiders developed plans in advance to harm the organizations. Forty percent of the cases involved overt behaviors in preparation for the incidents. In 15% of the cases, the overt behaviors were technical actions taken to set up the attacks.

Fifty-five percent of the insiders came to the attention of someone for behavior of concern or behavior that was inappropriate prior to the incidents. These behaviors included, among others, patterns of tardiness, absenteeism, arguments with coworkers, and poor job performance. Of those cases, the following conditions were observed:

- In 97%, the insider's behavior(s) came to the attention of others in the workplace, including supervisors, coworkers, subordinates, and executives.
- In 70%, the insiders were reprimanded in the workplace for their behaviors.

In 46% of the cases, other individuals had information about the insiders' plans, intentions, and/or activities prior to the attacks. In these cases, "others" included

- coworkers (32%)
- acquaintances (20%)
- family members (16%)
- friends (12%)
- individuals who were involved in and benefited from the attacks (64%)
- and, in 36% of these cases, multiple individuals had at least partial knowledge of the insiders' intentions, plans, and/or ongoing activities.

Behaviors and information known by other individuals prior to the attack included the following:

- Insiders told coworkers, supervisors, and family members directly that they planned to shut down their companies or the companies' systems or had already taken steps in preparation to take down the systems.
- Insiders told or showed coworkers how fraud or other damages to the organizations' systems could be easily committed.
- Insiders were physically observed in unusual places for their positions, including entering restricted areas of buildings or entering office spaces that were atypical for them and sitting at coworkers' desks and workstations while the coworkers were away from their offices. In some cases, these activities were observed on more than one occasion and in one case an insider was observed in an unusual area five to six times in one day.
- Insiders made attempts to get coworkers to help with copying files and data or gaining access to accounts outside the scope of the insiders' responsibilities.

In 44% of the cases, the insiders' pre-attack activities were noticeable, and could have been flagged as being suspicious either through on-line automated security programs or by other persons. In those cases, the insiders' planning activities were noticeable online (52%), offline (12%), and, in some cases, both online and offline (36%).

Insiders' on-line activities that may have been noticeable prior to the incidents included

- creating false client accounts and files on systems
- constructing and testing logic bombs
- centralizing critical assets
- sabotaging backups
- downloading malicious code or materials[34]

Thirty-six percent of the insiders communicated to others negative feelings, grievances, and/or interest in causing harm. In 42% of these cases, the insiders communicated their negative sentiments about the affected organizations or individuals directly to these organizations or individuals, and in 53% of the cases, they communicated these sentiments to someone else. Insiders communicated these negative sentiments in various ways, including verbally (92%) and via email (12%).

Twenty-seven percent of the insiders examined had a record of disciplinary actions within the organization prior to the incidents,[35] and 29% had experienced changes in their employment performance or had disciplinary problems prior to the incident.

Advancing the Attacks

> *The sole system administrator at an organization in the IT sector quit his job with no notice to his employer. Prior to leaving his position, the insider changed all of the passwords on the organization's systems and then refused to provide the system administrator passwords to his former employer until he received pay for his last two days on the job. During that time period he also changed the IP address for the company's DNS server so that no one could access the company website. The entire company was locked out of the system for two days, until the former employer finally paid the insider the money that he was demanding.*

Key Findings

- Half of the insiders had authorized access to the systems/networks at the time of the incidents.
- Over half of the insiders used relatively sophisticated tools or methods for their illicit activities, including scripts or programs, autonomous agents, toolkits, probing, scanning, flooding, spoofing, compromising computer accounts, or creating unauthorized backdoor accounts.
- Over half of the insiders exploited systemic vulnerabilities in applications, processes, and/or procedures.
- Insiders committed their illicit activities from within the workplace or remotely in nearly equal numbers.
- The incidents took place during and outside normal working hours in nearly equal numbers.

[34] While we only have data on this topic for half of the cases, we know that in 27% of those cases the insiders had a history of keeping malicious materials (code, source code, or tutorials) on their computers.
[35] Data were only available for 48 of the 57 insiders.

Supporting Data

Half of the insiders had authorized access to the systems/networks at the time of the incidents. In 29% of the cases, the insiders' access had been disabled by their employers prior to the incidents. In 23% of the cases, insiders were able to carry out their illicit activities after their termination because their employers did not disable their access.

Fifty-eight percent of the insiders used one or more relatively sophisticated methods of attack,[36] including

- a script or program
- an autonomous agent
- a toolkit
- probing
- scanning
- spoofing
- compromising an account
- creating unauthorized backdoor accounts.

In 38% of the cases, the insiders compromised an account to carry out the incidents. These compromises included the use of another's username and password (30%) or the use of an unauthorized account created by the insiders (12%).[37] In 86% of these cases, there were no indications of suspicious activity related to the accounts before the attacks were initiated.

Twenty-three percent of the insiders used shared accounts to carry out their activities, including group accounts, e.g., system administrator or database administrator (DBA) accounts (19%), and company accounts (4%). In 56% of the cases, the insiders used their own usernames and passwords. In 21% of the cases, the insiders used accounts in more than one of the above categories to carry out the incidents.

In 62% of the cases, the insiders exploited or attempted to exploit systemic vulnerabilities in applications, processes, and/or procedures (e.g., business rule checks or authorized overrides).

In 42% of the cases, the insiders' actions were limited to relatively unsophisticated methods of attack. These methods included user commands, information exchanges, and exploitation of physical security vulnerabilities.

Although data were only available on 37 organizations, 86% of those organizations permitted employees remote access.

[36] Most of the insiders did not show an interest in, possess materials on, or engage in "hacking."

[37] Two insiders used another's username and password, and created unauthorized account(s).

In 43% of the cases, the attacks were conducted from outside the workplace via remote access, 51% took place only from within the workplace, and 6% took place both from within the workplace and remotely.

Forty-nine percent of the attacks took place outside of normal working hours or on weekends or holidays, and 51% took place during normal working hours. Some incidents were carried out from multiple locations, both during and outside working hours.

The table below describes the time and location of the incidents in more detail.

	At the Workplace	Outside the Workplace
During Working Hours	35%	19%
Outside Working Hours	22%	29%

Time and Location of Incidents

Eighty-eight percent of the insiders who used remote access for their attacks were former employees.

Thirty-one percent of the insiders were granted system administrator access upon hire. At the time of the incidents, however, none of them had authorized administrator/root access.

An additional 42% of the insiders were hired as privileged users, and 65% of them retained authorized privileged access at the time of the incidents. At the time of initial hire, of the insiders with authorized privileged access or authorized administrator/root access, 19% held professional, administrative, clerical or service positions, and 33% held technical positions.

Detecting the Attacks

> *Two days before he resigned to begin a new job with a competitor, a member of a product development team stayed at the office after hours and downloaded hundreds of confidential files for projects to which he was not assigned from the company's server onto his desktop computer. He then copied the files to CDs and deleted the files from his desktop. An investigation of the insider's activities was initiated after he left for his new job when his former employer examined the logs on his desktop computer and noticed the large number of file deletions. His new employer cooperated with federal authorities and provided access to the insider's work computer. Although none of the files were found, the new employer's system backups showed that the files had in fact been on the insider's desktop computer. The insider had deleted these files when he became aware of the investigation. There was no financial damage incurred by either organization.*

Key Findings

- Most of the insider attacks were only discovered through manual (non-automated) detection of an irregularity or failure of an information system.
- System logs were the most prevalent means by which the insiders were identified.
- The majority of the insiders took steps to conceal their identities and their activities.
- Most of the incidents were detected by non-security personnel.
- The majority of attacks were accomplished using company computer equipment.

Supporting Data

Eighty-six percent of the incidents were detected only after there was a noticeable irregularity in an information system or a system became unavailable.

Eighty percent of the incidents were detected through manual procedures only, and 16% were identified using a combination of automated and manual procedures. Twenty-four percent of the incidents were detected through observation and notification by others.

The various mechanisms used to identify the perpetrators included

- system logs (67%)
- forensic examination of the targeted networks, data, or systems (35%)
- the insiders' own source IP addresses (33%)
- username (25%)
- phone records (22%)
- forensic examination of the insiders' home computer equipment (18%)

Of the 67% of cases in which system logs were used to identify the insider as the perpetrator, the following types of logs were used:

- remote access logs (52%)
- file access logs (52%)
- database/application logs (32%)
- system file change logs (29%)
- email logs (23%)

In 61% of those cases, multiple types of logs were used to identify the insider.

In 74% of the cases, the insiders took steps to conceal their identities (21%), actions (21%), or both (32%). These insiders engaged in activities to conceal their identities and/or actions, such as

- using technology to delete or modify records of the incidents (38%)
- denying their part in the activities (36%)
- using a false name/organization (17%)
- using another person's password (14%)

- using another's terminal, creating unauthorized accounts/backdoors, using a third party to carry out the incident, or actively diverting suspicion in the direction of others (10%)

Half of the insiders engaged in more than one type of method to conceal their actions, identities, or both.

Seventy-four percent of the incidents were detected by individuals who were not part of the organizations' security staff.[38] These individuals included customers (20%); supervisors (20%); and other non-security personnel (44%).

In those cases where the attacks were detected by security personnel, the incidents were uncovered by a range of security professionals, including IT security staff or system administrators (20%), and staff responsible for information systems/data (4%).

In 64% of the cases, the insiders used company computer equipment to access information for the attacks. In 41% of those cases, the insiders used computer equipment assigned to another employee, group of employees, or department within the target organizations.

The Consequences of the Attacks

For the Insiders

> *After being fired for non-performance, an insider repeatedly accessed his former company's systems to view former coworkers' email accounts and proprietary source code information. As a result of these actions, the insider was convicted on charges of computer theft, accessing a computer system, and unlawful access to stored communications. The insider was sentenced to probation and ordered to pay restitution to the target organization. The insider stated that he had been checking on the status of a project in which he had invested a lot of work and time, and was not trying to steal trade secrets from, or otherwise harm, the target organization. Furthermore, the insider asserted that he did not think what he was doing was criminal.*

Key Findings

- Most of the insiders did not consider the severity of the consequences that could result from their actions, to include personal and professional costs.
- Almost all insiders were charged criminally, the majority of which were charged with violating a federal or state computer-related criminal statute.
- The majority of the insiders charged with criminal offenses faced multiple punishments.

[38] Note that in most cases the insiders were detected by multiple people.

Supporting Data

Most of the insiders (85%) did not take into consideration the severity of the consequences that could result from their actions.

Ninety percent of the insiders faced formal criminal charges. Of these, 51% faced federal charges, 47% faced state charges, and 2% faced both federal and state charges. In 50% of these cases, the insiders were charged with a federal violation of unauthorized computer use or intrusion (18 USC 1030), 16% were charged with a state computer-related offense, 16% were charged with a non-computer related state offense, and 18% faced various other charges.

Of those insiders who faced criminal charges, 84% were adjudicated guilty at trial or under a plea agreement; 4% entered a plea of no contest; and 12% involved a variety of other dispositions. Seventy-seven percent of these insiders were sentenced to probation or supervised release; 48% were ordered to pay restitution; and 46% were sentenced to a period of incarceration.[39] Sixty-one percent of the insiders received multiple punishments.

Average sentences imposed upon conviction of insiders for their acts included

- incarceration for periods ranging from 1 to 96 months, with an average incarceration period of 19 months
- probation for periods ranging from 12 to 180 months, with an average probation period of 45 months
- restitution in amounts ranging from as low as $100 to as high as over $7 million

There were a variety of personal and professional costs incurred by insiders:

- termination from job(s)
- difficulty finding future employment
- restricted future computer use, including forfeiture of the right to own a personal computer system or use the Internet
- financial penalties, such as several years of restitution
- restrictions on mobility that include travel only within an approved area

In all of the insider cases, the organizations responded to the incidents by taking action external to the organizations. Almost all (94%) of the incidents resulted in law enforcement notification or the filing of a civil lawsuit (15%).

In those cases in which law enforcement was notified, organizations contacted

- federal law enforcement agencies and/or U.S. attorneys' offices (39%)
- local police departments and/or local prosecutors' offices (35%)
- state law enforcement agencies and/or state prosecutors' offices (12%)
- two or more of these groups (e.g., local and state police departments) (14%)

[39] Some insiders suffered multiple consequences; total exceeds 100%.

For the Target Organizations

> *A network administrator, who designed and implemented his company's email server, became disgruntled with his employer and left the company when he was offered substantially more money by another firm. Upon leaving, the insider was permitted to retain access to his former email account, per company policy. He exploited that privilege to cause the email server to crash. The insider's former employer then requested the insider's assistance to restore the server. In the process of restoring the server, the insider installed a modem on the system which he used later to cause even more damage to the organization, to include*
>
> - *perused internal executive email*
> - *forwarded information on new hire compensation to current employees*
> - *attempted to dissuade new hires from joining the company*
> - *forwarded internal executive discussions to current employees*
> - *forwarded information about employee disciplinary discussions to employees*
> - *disclosed employee bonuses and raises*
> - *passed company information to former employees*
> - *passed internal discussions and bid information to competitors*
>
> *The company subsequently went out of business, estimating that it incurred damages in excess of $7 million from the insider's actions.*

Key Findings

- Insider activities caused financial loss for organizations, negative impacts to their business operations, and damage to their reputations.
- Incidents affected the organizations' data, systems/networks, and components.

Supporting Data

Eighty-one percent of the target organizations experienced a negative financial impact as a result of the insiders' activities. The dollar amount of these losses ranged from a reported low of $500 to a reported high of at least $20 million. In 17% of cases, there was no reported financial damage to the organization; and in one case, the financial damage to the organization was unknown. A table representing the percentage of organizations that experienced financial losses within broad categories is provided in Appendix B.

Of the 81% of organizations that suffered financial damage, 71% incurred financial damages less than $400,000, and 29% incurred financial damages above $400,000. In cases where financial damage was less than $400,000, employees primarily held technical positions (80%). In the majority of cases where financial damage was over $400,000, employees held non-technical positions (75%).

Fifty-two percent of the examined organizations experienced some impact on their business operations, including

- interruption of affected organizations' ability to conduct business due to shut-down of networks, routers, servers, or dial-up access
- blockage of customer contact with the affected organization due to modified or deleted customer information
- damage to or destruction of critical information assets, such as proprietary software, data, computing systems, and storage media necessary to the organizations' ability to contract work, produce product, or develop new products
- failure of mission critical operations due to modified or deleted software applications

Forty-one percent of the organizations experienced a negative impact to their reputations. Examples of the effects on the target organizations' reputations in these cases include

- negative media attention received regarding the incident
- derogatory information about the company sent from an insider to customers and employees in email communications
- personal or private data of customers or employees posted on web sites or sent in emails
- customer businesses affected during the incident
- company web site defaced
- company services became unavailable to clients

Twenty-seven percent of cases involved either intentional or unintentional harm to a specific individual. Examples of harm inflicted by insiders on coworkers, supervisors, or company owners include

- threatening either physical harm or another type of consequence
- implicating others not involved in the incidents
- targeting the credit records or personal finances of others

Ninety-six percent of the incidents affected the integrity, confidentiality, and/or availability of the organizations' data. In these incidents, the insiders inflicted harm by

- modifying and/or deleting data (71%)
- corrupting data (56%)
- reading, copying, and/or stealing data (48%)
- engaging in unauthorized disclosure of data (38%)

Fifty-two percent of the incidents affected the integrity, confidentiality, availability, or authentication of the organizations' information systems/networks. The insiders' attacks in these incidents included denial of service in 48% of the cases; unauthorized increase in system/network access in 25% of the cases; and theft of resources in 29% of the cases. Thirty-eight percent of the incidents targeted the organizations' network, components, or external connectivity.

Of those cases involving theft of intellectual property, information stolen included not only source code and system design information, but also data for which the organization was responsible. The types of information stolen in these cases included

- customer information
- social security numbers
- financial account numbers, including credit card numbers
- project ideas, descriptions, requirements, specifications, designs, and proprietary information for new products under development
- source code for the company’s primary products
- pricing information for outside bids

Section 3: Implications of the Key Findings for the Prevention of Illicit Insider Cyber Activity in the IT Sector

In this section, the authors discuss key findings of the study of illicit insider cyber activity in the IT sector and their implications for developing strategies for the prevention of such incidents.

The discussion of implications is organized under three categories: The Insiders, The Attacks, and The Consequences of the Attacks. Presented under each category are the key findings and the implications. The implications are followed by a commentary that describes them in greater detail.

The Insiders

Key Findings

Characteristics

- Current and former employees carried out illicit insider activities in nearly equal numbers.
- Most insiders were either previously or currently employed full-time in a technical position within the organization.[40]
- Thirty-eight percent of the insiders had been arrested previously.[41]
- Insiders represented a wide range of ages, from 17 to 58 years.[42]
- Insiders represented a variety of racial and ethnic backgrounds.
- The majority of insiders were single at the time of the attack.
- Insiders predominantly were male.

Motives

- A specific event or series of events triggered most insiders' actions.
- Multiple motives were reported for the majority of insiders. Revenge was reported as the main motive in just over half the cases.
- The most frequently reported goals of insider attacks were financial gain, theft of information/property, and sabotage to the organization.

Implications

- Insiders did not share a common profile.
- Pre-employment screening may be useful.
- Management attention to employee issues may help to diffuse potential harm.

[40] A technical position is one requiring specialized skills in computer science or information technology, including programming, scripting, networking, information security, or system architecture and configuration.

[41] Data were only available for 47 of the 57 insiders studied.

[42] Data were only available for 48 of the 57 insiders studied.

Insiders did not share a common profile. A wide variety of individuals perpetrated the insider incidents in the cases studied. Although the majority of insiders were employed in technical positions, 37% of the insiders held other administrative, professional, or management positions. Insiders in both technical and non-technical positions were granted privileged access to systems. Overall, in these reported cases, insiders in the non-technical positions caused greater financial damage to the organizations.

The status of the employee's position, whether current or former, was not a factor in perpetrating the attacks. Both current and former employees committed insider acts in nearly equal numbers. Insiders were demographically varied with regard to age and racial and ethnic background. The majority of insiders in this sector were not perceived by co-workers to be disgruntled employees, although the study found that many did hold a work-related grievance prior to the incident.[43]

These findings suggest that whether an employee occupies a technical or non-technical position may be less important than whether they have privileged access to systems. These findings also suggest that perceptions regarding disgruntled employees or technical staff members being likely to pose the greatest insider threats may be inaccurate. Instead, identifying prior concerning behavior(s) and employment histories may be more helpful than relying on stereotypical perceptions.

Pre-employment screening may be useful. In the IT sector, the findings suggest that although pre-employment or background checks were conducted by some organizations, they were not common practice for all companies.[44] In addition, thirty-eight percent of insiders had a prior criminal record that involved arrests and convictions for substance abuse, fraud, larceny, and aggravated assault. Of those insiders with prior criminal histories, over half had multiple prior arrests and convictions.

These findings underscore the importance of knowing the type of person who ultimately will be entrusted with privileged information and/or access within the organization. Pre-employment checks may uncover information about the character and prior behavior of potential or current employees that can inform decisions regarding access to privileged information. Simple reference checks or basic criminal history checks for prospective or current employees may help identify individuals with histories of fraud, theft, or other concerning behavior.[45] In the cases examined in this sector, knowledge of these prior behaviors or criminal acts may have precluded some organizations from granting privileged access to individuals who ultimately harmed the organization.

[43] Also, as previously noted, there was no evidence that insiders showed an interest in, possessed materials on, or engaged in "hacking."

[44] Data were only available for 37 of the 52 cases. Of those, 52% of companies conducted background checks on employees, contractors and others; 49% of the companies did not conduct background checks.

[45] In one case, an individual used a false social security number which prevented the organization from finding the true criminal history when they did conduct a background check.

Management attention to employee issues may help to diffuse potential harm. The majority of insiders in this sector experienced a specific job-related event or series of events that played a part in triggering the incidents. These events included negative work-related situations, employment with a new company, and circumstances in which pressure from, or anger towards, other individuals outside the working environment spurred the insider to carry out the activities. The primary motives and goals of these insiders included revenge against supervisors, coworkers, and company owners; financial gain; and theft of intellectual property.

These findings suggest that organizations may benefit from reviewing existing, or developing new, policies and procedures to guide management and employees in how to handle sensitive issues. Particularly, providing guidance and encouraging management to pay attention to employees who experience negative employment-related events including employment termination, demotion, or conflicts with coworkers and management may be helpful. Management should exhibit interest in, and create opportunities to, address employee concerns, grievances, complaints, or other issues in an effort to decrease employee dissatisfaction or other negative affects. These interactions with employees may provide company officials clues as to whether an employee may be contemplating doing harm to the organization, and opportunities to defuse potentially destructive and costly situations.

The Attacks

Pre-attack Behaviors and Planning

Key Findings

- The majority of insiders planned their activities in advance.
- The majority of insiders came to the attention of someone in the workplace for problematic or unusual behavior prior to the incidents.
- Others had information about the insiders' intentions, plans, and/or ongoing activities.

Implications

- Opportunities exist to uncover employee intentions.
- An environment that encourages employees to report their concerns, suspicions, or observations of unusual behavior is important.
- Reports of problematic behavior should be documented and procedures should be developed to respond to such reports.

Opportunities exist to uncover employee intentions. The findings suggest that there may be opportunities for company personnel to discover an individual's intentions prior to the harm. The majority of insiders in this sector planned their activities in advance. In addition, in many cases, others were aware of the insiders' plans or the employees' unusual activities were noticeable prior to the incidents.

Many of the cases involved communications with coworkers and management regarding the insiders' plans, or coworkers observed unusual activities by the insiders that aroused their suspicions. In several known cases, coworkers, supervisors, family, or friends had knowledge about the insiders' concerning behavior or actual plans that was not shared until an investigation of the harm was initiated. All levels of company personnel have the opportunity to discover information that may help stop harmful activity to an organization before it occurs.

An environment that encourages employees to report their concerns, suspicions, or observations of unusual behavior is important. Over half of the insiders in this sector came to the attention of someone in the workplace prior to the incident for behavior of concern, including inappropriate behavior or aggressive behavior towards others; poor work habits; and obvious extreme dissatisfaction with the organization. The study found that in several cases within this sector, information emerged that indicated employees of the target organizations had been uncomfortable or unwilling to come forward to management with the information they knew or suspected about the insiders. Encouraging employees to report behavior of concern, particularly in cases where they may have suspicions of illicit activity, is important. Of equal importance is creating a culture where employees understand the key role they play in helping to identify and stop potential malicious insider activity.

Reports of problematic behavior should be documented and procedures should be developed to respond to such reports. A formal procedure should be developed to ensure that relevant information concerning problematic behavior of employees is gathered and documented in a standard and thorough manner. Such documentation will serve to create a recorded history of various concerning behaviors that, in turn, will provide company officials with the ability to track the course of behavior over time and produce a recorded basis for disciplinary action, if such action is warranted. In addition, appropriate procedures should be developed that allow various departments within the organization to share information regarding problematic or suspicious employee behavior. Representatives from management, security, information technology, human resources, and legal counsel would benefit from sharing information that they have learned regarding particular behaviors of concern.

Likewise, developing a formal process for all employees to report problematic behavior in the workplace is important. An established procedure that can be followed in a responsible and professional manner will lay the groundwork for fair and responsive action by the organization. This procedure also will inform employees that the organization has developed specific ways to address concerning behavior in the workplace, which may encourage their reporting of such behavior and possibly serve as a deterrent to potential illicit insider activity. Finally, company officials may wish to consider instituting a mechanism that will permit employees to report problematic workplace behavior anonymously.

Advancing the Attacks

Key Findings

- Half of the insiders had authorized access to the systems/networks at the time of the incidents.
- Over half of the insiders used relatively sophisticated tools or methods for their illicit activities.
- Over half of the insiders exploited systemic vulnerabilities in applications, processes, and/or procedures.
- Insiders committed their illicit activities from the workplace and remotely in nearly equal numbers.
- The incidents took place during and outside normal working hours in nearly equal numbers.

Implications

- Access controls should limit an employee's access to proprietary information to only that information that he or she requires to perform assigned tasks.
- Comprehensive password policies, procedures, and technical controls should be implemented and communicated to employees.
- Comprehensive computer account management policies and practices should be implemented.
- Formal policies and procedures for disabling access - both physical and electronic - upon an employee's termination or resignation should be established and followed.
- Procedural and technical controls should be established for system administrator functions.
- Configuration management practices should be established and enforced to prevent or detect release of malicious code or system modifications.

Access controls should limit an employee's access to proprietary information to only that information that he or she requires to perform assigned tasks. The ITS found that lack of or insufficient electronic and/or physical access controls in the IT sector can facilitate an insider's illicit activity. For example, one insider was observed by a supervisor after working hours reading a coworker's email on the coworker's computer, which was left logged in. The supervisor told the insider to leave the facility. Instead, the insider proceeded to download and take proprietary materials from his place of employment with him, and also deleted logs that could have been used as evidence against him. Mandatory password-protected screensavers can eliminate this type of physical access vulnerability.

Organizations can reduce their risks of theft of proprietary information, sabotage, and fraud by <u>fine-grained access controls</u> - limiting access for each employee to only the information required to do his or her job.[46] These controls limit the damage one insider

[46] The coarseness level of access control restrictions is a relative measure. For example, user group level access control is coarser than individual user level access control. For example, user level access control

can inflict if he or she becomes disgruntled or otherwise decides to exploit the organization for personal gain.

In some cases, the ITS also found that insiders in the IT sector who had changed positions within an organization were able to commit acts of sabotage by retaining system access that was granted to them in their former positions. This oversight can result in a single employee being authorized for multiple roles, including approval and oversight, thereby circumventing separation of duties enforced via role-based access. Role-based access is an effective mechanism for enforcing separation of duties and fine-grained access controls, but requires diligence by the organization to ensure that the roles are maintained and monitored closely.

Proprietary or confidential information stolen in cases in this study ranged from source code and designs for new products under development to customer lists and sales strategies. Some insiders in this study were able to steal information to which they should not have had access in the first place. For example, one insider was a sales representative, but was able to download all of the source code for a new security product being developed by his company. Other insiders were able to steal information for entire projects because their access was not limited to the portion of the projects on which they were working.

System and network configurations also have implications for access control. One insider was able to exploit the trusted host configuration for the company's servers to obtain unauthorized system administrator access to three other servers. He used that access to plant a logic bomb on all three servers that deleted all of the files on each machine every Wednesday at three o'clock in the morning. The script executed successfully twice, requiring five days to recover, before a consultant discovered the source of the problem.

Comprehensive password policies, procedures, and technical controls should be implemented and communicated to employees. Insiders used another's username and password in almost one-third of the cases examined in this sector. Compromised accounts included login accounts as well as remote access/Virtual Private Network (VPN) accounts for coworkers, supervisors, customers, a senior manager, a vice president of sales, a chief financial officer, and a chief operating officer. Some insiders compromised multiple accounts. One insider, who left his job on a software development team to work for a subsidiary of the company, accessed 16 different computers of his former employer using at least 24 different accounts during the first month after leaving.

is tighter (more fine-grained) than group level access control. Another example, unconstrained remote access is coarser than remote access limited to non-critical functions. In general, coarse access controls are coarser than fine-grained access controls is more restrictive than unconstrained remote access.

Analysis of compromises in this sector suggests that formal policies should prohibit sharing of passwords and require the selection of strong passwords.[47] A procedure can be instituted, whereby attempts by anyone to obtain passwords would be reported and investigated immediately. In addition, organizations can educate all employees about the importance of protecting all of their passwords.

Implementation of obvious default password algorithms should be prohibited, and technical controls imposed to force password changes upon initial use. Organizations also should consider instituting policies, procedures, and technical controls to ensure confidentiality not only of their employees' passwords, but also of any external users with legitimate access to their systems. One insider stole passwords for external customers before resigning his position and working for a competitor. He then used those passwords to log into customer accounts on his former employer's system.

Comprehensive computer account management policies and practices should be implemented. Over three-fourths of the insiders who used someone else's account for their illicit activities were former employees at the time of the incidents. The absence of accurate documentation of all accounts to which an employee has access can make it difficult to completely disable that employee's access upon termination. The ITS findings suggest that organizations tend to create accounts and grant access to shared accounts on an ad-hoc basis, perhaps requiring formal authorization for privileged access, but not necessarily tracking that access once it is granted. Employees typically are assigned a computer account when they begin employment. However, additional accounts, such as remote access accounts; company intranet accounts; and administrative systems accounts (for example, shared calendar systems, and travel systems), frequently are created at a later date as needed.

Furthermore, system administrators and privileged users often are given passwords for multiple shared accounts on an as needed basis. Since passwords often are shared verbally, there may be no record of exactly which employees know passwords for each shared account. Organizational networks can be large, with hundreds or thousands of servers running hundreds of applications. This situation can result in the creation of many system administrator and privileged accounts, each shared among a different set of users. For example, system administrator functions across a large network can be divided geographically or along organizational lines, and database administrator (DBA) accounts can be shared among individual project teams or centralized teams of DBAs.

In addition to tracking authorized access to legitimate accounts, account management practices also should be instituted to detect the creation of unauthorized accounts. Some insiders created unauthorized, backdoor accounts that they later used to commit their attacks. These attacks, planned and executed by users with system administrator privileges, were harmful and difficult to trace. Illicit acts usually can be associated with

[47] Some passwords can be authorized for limited sharing but with individual accountability, for example, system administrator passwords. Passwords for individual accounts should never be shared. For a discussion regarding what constitutes a "strong" password see: http://www.cert.org/homeusers/HomeComputerSecurity/#6

the computer accounts used to commit them; however, backdoor accounts, because unauthorized and not tied to a legitimate user, do not provide clear, traceable paths back to those persons using them.

Periodic account audits should be conducted to check for unneeded or unauthorized accounts, including

- remote access accounts
- login accounts
- DBA accounts
- other application, customer, and company accounts

The audit should include verification by all account owners so that unauthorized accounts are discovered before they are used for illicit activity.

Formal policies and procedures for disabling access - both physical and electronic - upon an employee's termination or resignation should be established and followed. The absence of, or non-compliance with, formal policies and procedures for disabling an employee's access upon his or her termination or resignation was an enabler in many of the insider incidents examined by the ITS. In total, 47% of the incidents examined in this sector were carried out by former employees. Thirty-one percent of the insiders were granted system administrator access upon hire. At the time of the incident, however, none of them had authorized administrator/root access.

Almost one-fourth of the insiders who were former employees were able to carry out their illicit activities because their physical or electronic access to the organizations' systems or networks was not disabled. Furthermore, almost all of the insiders who used remote access for their illicit activities were former employees. Almost one-third of the insiders were able to carry out their actions even though their access had been disabled upon termination or resignation.

Finally, 10% of the cases in this report involved illicit activities committed by insiders after they turned in notices of resignation or were informed that their employment would be terminated, but prior to termination.

Collectively, these findings suggest that organizations should assess their termination policies and processes, particularly for termination of employees with elevated system access. Organizations may prevent such attacks by establishing formal policies and procedures for disabling access to the network upon an employee's departure.

Incomplete, ad-hoc, or outdated termination policies and procedures may increase the risk of access control gaps inadvertently left open for terminated personnel. Insiders' knowledge of the organizations' policies, procedures, technologies, and physical security measures provides them an enhanced ability to attack the organizations even when their access had been disabled. For example, one company disabled a terminated insider's access to the company's network, but overlooked disabling the password to the voice mail system.

The disabling of computer accounts, system authorizations, remote access, and physical access should occur immediately when employment, consulting, or contracting agreements are terminated, regardless of the reason for the termination. Employee and contractor termination procedures must include account audits conducted immediately prior to, and following, termination to check for unneeded or unauthorized accounts, and disabling access to *all* accounts to which that user had access, including shared accounts. An oversight exposes the organization to a vulnerability easily exploited by a former employee or contractor possessing the shared password.[48]

Termination procedures also should consider accounts that the organization has established with external organizations to which the former employee had access. For example, one insider had access to one of his organization's supplier's systems for purchasing computers and accessories for his organization. Following termination, he purchased equipment for his personal use, using the credentials of his former employer.

Procedural and technical controls should be established for system administrator functions. Insiders in this sector used another's account and password in almost one-third of the incidents. System administrators are responsible for such functions as creating accounts and setting default passwords. Consequently, it is important that procedural and technical controls be implemented for system administrator functions to prevent insiders from taking preparatory technical actions to set up future illicit acts.

Almost one-third of the insiders who perpetrated acts examined in this sector were granted system administrator access when hired. At the time of the incidents, none of them retained that level of access having terminated their employment, either voluntarily or involuntarily. Nevertheless, most of these insiders were able to perform their illicit acts due to their elevated access level by

- using others' accounts and passwords
- using shared accounts, including system administrator accounts
- creating unauthorized accounts for later use

Moreover, all but one of the insiders hired with system administrator access used technically sophisticated tools or methods for their activities. Risk of these types of attack methods and tools can be mitigated by technical controls to enforce separation of duties and two-person control for system administration functions. Such controls would reduce the risk of execution of those types of tools by a single insider, requiring collaboration among multiple employees with the necessary access levels. In addition, these controls mitigate the risk of a single omnipotent system administrator who has the ability to take control of the entire system.

Procedural and technical controls should be implemented and enforced to ensure that all actions, including the use of shared privileged or system administrator accounts, can

[48] Although information was available only for 26 cases, of those, 65% involved victim organizations that did not change group passwords for shared accounts, including system administrator accounts, upon an employee's departure.

be traced back to an individual user. System administrator accounts as well as some other types of shared accounts, such as database administrator accounts, are often shared by multiple users, and may be particularly vulnerable to insider misuse. Shared accounts were used in almost one-fourth of the incidents examined in this sector. It is important that systems be configured so that such accounts can be shared as necessary, but with individual accountability.

Configuration management practices should be established and enforced to prevent or detect release of malicious code or system modifications. Some incidents examined by the ITS arguably could have been prevented if more technical controls had been implemented for releasing changes to the organizations' production environments. For example, some insiders used scripts (including logic bombs) and/or autonomous agents to delete or corrupt critical files. Others released changes to the companies' websites that were immediately obvious and potentially harmful to the companies reputations. Another insider downloaded and installed a new application on the company's network that drastically impacted customer response times, while another was able to modify critical production applications.

Such technical attacks are stealthy and can be difficult to prevent. However, organizations can implement configuration management systems to reduce their risk by enforcing a two-person rule for releasing any changes to the production environment. Configuration management systems can be used to ensure that all changes to the production environment are fully tracked, and that approval by a second user with a designated approval role is required. The system architecture also can be designed to minimize the risk of a system administrator compromising the approval account by using a separate staging machine with separate system administrators.

Nevertheless, configuration management systems alone are not sufficient for thwarting insider threats. If the approval process, although manual and technically enforced, becomes a procedural technicality that is performed without actual verification of what is being released, then the control feature of the configuration management system is overridden. One organization had put in place a configuration management system that tracked details of all changes released to the production environment, but did not require secondary approval for release. In addition, the change log was never reviewed. Therefore, the insider was able to release a change to the communications driver he was working on before he terminated his employment. The change was never detected and was not set to execute for approximately six months following the insider's termination. At that time his code began to randomly insert the letter "i" into the company's electronic computer communications streams. During the investigation the logs were reviewed, and the release of the code was discovered.

Detecting the Attacks

Key Findings

- Most of the insider attacks were only discovered through manual (non-automated) detection of an irregularity or failure of an information system.

- System logs were the most prevalent means by which the insider was identified.
- The majority of the insiders took steps to conceal their identities and their activities.
- Most of the incidents were detected by non-security personnel.
- The majority of attacks were accomplished using company computer equipment.

Implications

- Logging and monitoring can be used for proactive, possibly automated, detection by security staff rather than solely for identification of the perpetrator following an incident.
- Automated business rules to enforce two-person control for verification of critical system modifications could serve as both a preventative and detection measure.
- Providing company-owned and -controlled equipment for employees (at the office and at home) facilitates host-based countermeasures for preventing or detecting attacks.
- Physical and logical access controls should ensure user accountability for actions and protect system logs from attempts to conceal activities or identities.
- Forensic evidence should be preserved and law enforcement should be notified for investigation assistance.

Logging and monitoring can be used for proactive, possibly automated, detection rather than solely for identification of the perpetrator following an incident. Often, many of the insider attacks were discovered by non-security personnel, through manual detection of a noticeable irregularity or failure of a system. For example, in some cases, insider attacks were detected when website defacements were noticed by customers and others external to the company; employees or customers were unable to access the company's system or services; employees or customers received email containing sensitive company information or malicious information regarding the company; or auditors noticed data irregularities. In another case, an insider's theft of a company's intellectual property was discovered following notification by a competitor.

Many of the insider attacks took place remotely. The insider was identified in these cases using a combination of remote access logs, source IP address, and phone records. In some cases, system administrators were discovering the damage to the system at the same time that customers were discovering their inability to access it. In other cases, customers provided the target organization the initial alert that there was a problem. These findings suggest that more active monitoring of system logs by the security staff might facilitate detection of an incident before it becomes apparent to the organization's employees or customers. For example, one target organization quickly discovered an insider's theft of proprietary information when routine monitoring of FTP logs uncovered unusual download activity after hours.

Mechanisms for automated detection of precursor activity also can play a greater role in earlier discovery of insider threats. For example, characterizing software, hardware, and information assets, and tracking their modification would provide an automated method for flagging system changes. Characterization entails establishing a trusted baseline for each machine on the network; storing it in a secure location; and periodically comparing the current “footprint” or configuration of each machine with that baseline. Unexpected files or changes to files revealed by this comparison can then be analyzed to determine whether they are legitimate changes to the baseline or rather, malicious code.[49] The release process for any new files also should incorporate procedures for updating the trusted baseline.[50]

Characterization processes require a combination of automated logging and manual review for identification of malicious system changes such as logic bombs. Likewise, automated logging of account creations would facilitate detection of rogue accounts, but also requires a combination of automated and manual analysis mechanisms.

Anomaly detection tools that monitor and flag individual actions for user activity deviating significantly from a pre-defined profile may also be useful; however, these tools are known to be expensive to operate, only minimally effective, and not widely available.

For the foreseeable future, the early detection of insider incidents likely will be accomplished most effectively using a combination of automated tools for logging, monitoring, and flagging suspicious activity, together with manual diagnosis and analysis.

Automated business rules to enforce two-person control for verification of critical system modifications could serve as both a preventative and detection measure. Some of the insider incidents examined for this report could have been prevented, or at least detected earlier, by automated business rules for notification and verification of critical system changes. For example, one insider who had access to the company’s personnel system defrauded that company of approximately $198,000 over a period of nearly 10 months. Three other insiders committed fraud within a large company by submitting false insurance claims totaling almost $850,000; payments against these claims were mailed to the insiders’ home addresses. In both cases, automated business rules could have facilitated early detection of these insider attacks. Notification of critical data modifications, particularly modifications to salaries, bank accounts, and addresses, could have been sent to a user with a verification role in the system or to the person for whom data was modified. Furthermore, employees’ awareness that this type of automated verification is in place could serve to prevent insiders from committing the fraudulent activity in the first place.

[49] Corporate Information Security Working Group Report of the Best Practices and Metrics Teams - Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee, United States House of Representatives November 17, 2004 (Revised January 10, 2005)
http://www.educause.edu/content.asp?page_id=666&ID=CSD3661&bhcp=1&bhav=6.00&bhsh=1024&bhsw=1280&bhiw=1278&bhih=848&bhqs=1

[50] For a complete description of security improvement practices for characterizing software, hardware, and information assets, see http://www.cert.org/security-improvement/practices/p091.html

Providing company- owned and - controlled equipment for employees (at the office and at home) facilitates host-based countermeasures for preventing or detecting attacks. Study findings that many insiders used company computer equipment to carry out their attacks suggest that host-based countermeasures installed on the equipment could be effective in preventing or detecting attacks. Such countermeasures could include access controls and attack detection techniques as described above. Companies that adopt such countermeasures should require employees to use company-provided equipment; limit the ability of employees to modify or disable the countermeasures; and prohibit storage of proprietary information on employees' personal computers.

Physical and logical access controls should ensure user accountability for actions and protect system logs from attempts to conceal activities or identities. In most of the cases examined, the insiders took deliberate steps to conceal their identities and/or actions. Investigators must be able to associate individual users with their actions. With this in mind, shared accounts should be used sparingly, if at all. In addition, because system logs were so crucial to the identification of the perpetrators, it is critical that these logs be secured from manipulation and backed up.

Investigators and organizational representatives should be cognizant during their investigation of incidents that insiders may attempt to conceal their identities and/or actions. Likewise, this potential insider behavior should be taken into account in configuring the network to effectively log future illicit activities and for tracing those activities to their sources. Many insiders used technology to delete or modify records of the incidents. Implementing physical and logical access controls to prevent such alterations will facilitate identification and potential prosecution of an insider should he or she be successful in carrying out an attack.

Forensic evidence should be preserved and law enforcement should be notified for investigation assistance. Forensic examination of computers in the workplace helped to identify some of the insiders, and forensic examination of the insiders' home computers helped to corroborate their identification. These findings suggest that information technology and telecommunications firms should establish policies and procedures for retaining system logs that potentially could be of use to investigations in the event of an insider attack. These policies should provide for retention of logs for a period long enough to ensure, with good likelihood, that an incident has not taken place. It also is critical for identification and successful prosecution that organizations contact a forensic specialist to advise the organization on maintaining the integrity of the evidence for law enforcement or other investigation.

The Consequences of the Attacks

For the Insiders

Key Findings

- Most of the insiders did not consider the severity of the consequences that could result from their actions, including personal and professional costs.
- Almost all insiders were charged criminally, the majority of which were charged with violating a federal or state computer-related criminal statute.
- The majority of the insiders charged with criminal offenses faced multiple sentences.

Implications

- Employee security awareness programs that highlight potential personal consequences may increase effectiveness.
- Developing policies and educating employees on ownership of intellectual property could assist in preventing illicit insider activity.

Employee security awareness programs that highlight potential personal consequences may increase effectiveness. The ITS findings suggest that the majority of insiders did not consider the *severity* of the consequences that could result from their actions. These consequences included not only legal actions against the insider, but personal repercussions as well. Of the insiders charged criminally, the majority were found guilty or pled guilty to the charges. Almost half the insiders were incarcerated for these crimes. The majority of insiders received multiple penalties for their actions to include incarceration, restitution, community service, and supervised release.

Personal repercussions that insiders suffered as a result of their actions included difficulty finding future employment; lost income; and negative affects on family. Specific examples include family members who were witness to the insider's arrest or insiders having to face the challenge of finding employment with a criminal record.

These findings suggest that in addition to developing policies and procedures outlining the types of actions which constitute illicit computer activity within the organization, companies may need to look beyond simply informing employees that certain activities are prohibited. Employee security awareness programs that communicate the extent to which an organization will pursue legal consequences for unauthorized use, and emphasize the personal and professional impacts that could result from illicit cyber activity may be more effective than those that do not. Creating awareness programs that encourage employees to think about the possible personal, professional or legal repercussions of unauthorized use may help to deter some activity.

Developing policies and educating employees on ownership of intellectual property could assist in preventing illicit insider activity. Information in this study was inconclusive regarding whether the affected organizations had formal acceptable use policies in place prior to the incidents. Researchers were able to determine, however, that in the theft of intellectual property cases, almost half (nine cases) of the organizations required the insider to sign a confidentiality agreement.

The insiders' intentions in the theft of intellectual property cases were unclear. Insiders in half of these cases stated that they intended to use information, programs, or data that they had created for their respective former employers as a personal resource to improve their performance at a new job, or to check on the progress of projects in which they previously had been involved. In a few cases, insiders believed they were helping a friend or acquaintance by sharing confidential client or company information with these individuals. They did not believe they were harming the company.

Researchers were unable to definitively state in the majority of these cases that the insiders intended to financially benefit or harm the organization, or had any other malicious intent.

For the Target Organizations

Key Finding

- Incidents affected the organizations' data, systems/networks, and components.

Implications

- Strict backup policies and procedures that are periodically tested can minimize the impact of an insider attack.
- Failover mechanisms should be implemented for critical systems that require high availability.

Strict backup policies and procedures that are periodically tested can minimize the impact of an insider attack. Almost all of the incidents examined for this report affected the integrity, confidentiality, and/or availability of the organizations' data, and half of them affected the integrity, confidentiality, or availability of the organizations' information systems or networks. More insiders modified, deleted, or corrupted information than simply copied, stole, or disclosed information. This report presents various suggestions for reducing the risk of unauthorized access or modification of critical data by insiders, as well as denial of service or sabotage of systems and networks. However, organizations still need to take steps so that they can recover as quickly as possible should an insider modify, delete, or corrupt critical data or systems.

Losses to organizations in this report ranged from a reported low of $500 to a reported high of at least $20,000,000. Some were able to recover fairly quickly from backups, while others required significant effort to resume normal operations. One former insider from a cable company deleted data and software used by the company to overlay local commercials into the broadcasts of more than one hundred channels. Unfortunately, when the company attempted to recover from the attack, their technical staff found that system backups were damaged, making recovery much more difficult. As a result, the company was unable to broadcast commercials for ten days, resulting in estimated loss of revenue of approximately $20,000 per day.

Quality backups not only provide a recovery mechanism, but also can provide a means for quickly determining exactly what damage was done by the insider. One organization noticed that a former insider had defaced the organization's website. By comparing the current system to the backups, the company personnel found other malicious activity that was not as obvious –the insider also had modified the billing database.

Finally, this report identified cases in which attackers deleted backups, stole backup media, or performed actions that could not be undone due to faulty backup systems. To guard against insider threat, organizations need to assure that backups are not only performed and periodically tested, but that the media and content are protected against modification, theft, or destruction.

Failover mechanisms should be implemented for critical systems that require high availability. Normal defensive measures, in particular backups, may not always be sufficient for recovery from insider attacks. Some of the insiders in cases examined for this report attacked mission critical systems that required a hot backup system for immediate failover. For instance, one insider crashed the system that provided immediate address information for emergency 911 calls based on the incoming phone number for emergency services. In that case, restoring the system from backups was an inadequate recovery mechanism. Unfortunately, in this case, the insider also stole the onsite and offsite backup tapes, making recovery even more difficult.

This report highlights the need for organizations to deal proactively with potential insider threats through ongoing risk analysis of survivability and resiliency of critical systems in the face of attacks by well-placed individuals. Critical networks, systems, and data must be carefully protected and appropriately validated at regular intervals. The degree of impact observed in these cases serves to justify the cost of such measures. For instance, one former insider deleted the system volume from the company's server that was used for interstate and foreign commerce and communications. This was the only means for the company's overseas office to access the company's business applications. The office could not enter orders, generate checks, or perform any other business transactions for the two and a half days that it took to recover the system.

Section 4: Conclusion: Reflections on the Findings for the Prevention of Illicit Insider Cyber Activity in the IT Sector

This section of the report reflects on certain aspects of insider activity that were more prevalent in this sector than in the study's previous examinations of insider attacks in the banking and finance sector and insider sabotage across critical infrastructure sectors. This paper reports findings regarding the type of incidents that occurred within the IT sector from 1996 to 2002; the types of vulnerabilities exploited by insiders with inherent knowledge of an organization's systems and networks; and information on the insiders' behaviors and activities prior to the actual incidents. These findings offer insight into illicit insider activity within the IT sector.

Illicit insider activity in the IT sector in particular serves as a prime example of the importance of educating and training all employees at every level of the organization in security awareness issues, acceptable use policies, and the key role each employee can play in the prevention and early detection of insider activities. Employees from clerical staff to high level managers in this sector observed unusual activity or were aware of an insider's plans, but for a variety of reasons, did not report this knowledge or their suspicions. Education that helps employees to recognize, and encourages them to report, concerning or unusual behavior is an important step in the early detection of insider activity. Creating a culture of security in which employees understand that they are an important line of defense against harmful and abusive attacks on systems and data is a key component of any strategy to mitigate the threat of illicit insider activity.

Furthermore, the findings in this report indicate that insiders frequently underestimated the possible consequences of their actions. In addition, some of the insiders who stole information, property, or data shared the information with others without malicious intent. Employees in this sector should be informed as to what type of activity constitutes illicit computer activity for the organization. Educating employees as to the consequences that could result from this type of activity, particularly the personal costs that could be suffered, is a tool that can be utilized to mitigate the risk of insider threat. Requiring employees to sign intellectual property agreements is another tool that may raise their awareness of the serious nature of taking information or data, while increasing an organization's chances for successful prosecution of these cases.

Pre-employment screening, particularly conducting background checks, is a preventive measure supported by study findings regarding the number of insiders in this sector that had prior convictions and arrests. While the number of insiders with criminal backgrounds was higher in the information technology and telecommunications sector, the ITS found that some of the insiders in each of its previous two studies had been arrested and convicted on criminal charges as well. Reference checks and criminal history checks can surface information that will help to inform risk-based decisions about who is being given access to critical systems and data within an organization.
In the IT sector, fifty-six percent of the insiders used their own usernames and passwords to carry out the attacks, suggesting that organizations should devote equal

attention to fine-grained access controls and account and password management practices to reduce chances for account compromises. Access controls must be carefully designed and closely controlled and monitored on an ongoing basis so that each employee's access is limited to only the information, applications, and systems that the employee has a legitimate need to access. Similarly, access within individual systems and applications must be strictly limited. These measures could enhance the ability of IT organizations to mitigate the risk of theft of intellectual property, which was more prevalent in this sector than in the previously studied sectors.

While access controls and account and password management provide several critical layers of defense against insider threats, these measures must be reinforced by close system monitoring. Ongoing monitoring increases the likelihood that if an insider succeeds in bypassing those controls, the malicious activity can be detected as quickly as possible and its impact contained. In the IT sector, the findings suggest that closely monitoring both activity within the workplace and remote activity are equally important since insiders committed their illicit activities from the workplace and remotely in nearly equal numbers.

The insider threat pervades all sectors, as do instances of each type of insider threat to include fraud, theft of intellectual property, and sabotage. The practices suggested in this report may be effective in facilitating the early detection or prevention of insider attacks. The ITS offers statistical evidence that can be used to justify the benefits of implementing such practices.

APPENDICES

APPENDIX A: Incident Date and Affected Headquarters' Locations

Reported Incidents by Year of Initial Damage

YEAR	NUMBER OF INCIDENTS
2002	5
2001	6
2000	9
1999	8
1998	10
1997	5
1996	9

Headquarters' Locations of Affected Organizations[51]

STATE	NUMBER OF INCIDENTS
California	14
Florida	3
New Jersey	3
New York	3
Pennsylvania	3
Washington	3
Minnesota	2
Ohio	2
Virginia	2
Colorado	1
Connecticut	1
Georgia	1
Illinois	1
Indiana	1
Kansas	1
Maryland	1
Massachusetts	1
Michigan	1
New Hampshire	1
North Carolina	1
South Carolina	1
Tennessee	1
Texas	1

[51] Data were only available for 49 of 52 incidents.

APPENDIX B: Organizational Size and Financial Damage

Size of Organizations by Number of Employees[52]

NUMBER OF EMPLOYEES	NUMBER OF ORGANIZATIONS
1 – 100	21
101 – 500	7
501 – 3,000	2
3,001 – 10,000	2
10,001 – 50,000	8
Over 50,000	5

Financial Damage Resulting From Incidents

DID COMPANIES EXPERIENCE FINANCIAL DAMAGE?	N=52	PERCENTAGE OF ORGANIZATIONS
NO	9	17%
YES	42	81%
DON'T KNOW	1	2%
FINANCIAL LOSS	**N=42**	**100%**
$1 to $20,000	17	40.5%
$20,001 to $50,000	4	9.5%
$50,001 to $100,000	3	7.1%
$100,001 to $200,000	3	7.1%
$200,001 to $300,000	3	7.1%
$300,001 to $400,000	0	0.0%
$400,001 to $500,000	5	11.9%
$500,001 to $1,000,000	1	2.4%
$1,000,001 to $5,000,000	2	4.8%
$5,000,001 to $10,000,000	2	4.8%
Greater than $10,000,000	2	4.8%

[52] Data were only available for 45 of the 52 cases studied.

APPENDIX C: Additional Case Examples

Pre-Attack Behavior and Planning

Others knew or suspected plans or intentions

Several days prior to accessing the company's network and deleting crucial files, the insider told a coworker that he put backdoors in the organization's systems and planned to use them to damage those systems. The coworker attributed the comment to what he characterized as the insider's usual strange behavior, and never reported the incident. In addition, after the insider attack occurred, several coworkers stated they had not reported the insider's unusual behavior because they were afraid of being targeted by the company and possibly fired.

* * * * * * * * *

Several days prior to an organization's system being sabotaged and taken down, the insider told a manager that he was going to shut the company down. It was widely known among management that there were behavioral issues with the employee. The insider's manager knew other steps were being taken to discipline the employee and did not report the threat. The attack occurred after months of unsatisfactory performance by the insider and, specifically, in retaliation for lack of payment of money that the insider alleged was owed to him by the company.

* * * * * * * * *

One week prior to an insider attack that brought an organization's system down, the insider told a company client who had previously worked for the company that he was going to take down the company's business. The client did not report the threat until after the harm to the organization occurred.

* * * * * * * * *

An insider requested a coworker's help in copying files from his hard drive to a disk. The request was not unusual and the coworker complied. After the insider left the company a week later, the coworker learned from the insider that he deleted everything off his hard drive to get back at the company and his boss. The coworker did not come forward until the insider's actions were discovered and an investigation commenced.

* * * * * * * * *

A supervisor showed a member of the IT team the ease with which fraudulent data could be entered into the organization's database. Although the co-worker thought activity was slightly odd she did not report the action. The supervisor then used the fraudulent data, which remained in the system, to carry out a fraud scheme against the organization.

* * * * * * * * *

An insider was observed utilizing the workstation of a vacationing employee who worked in another area of the organization. Other employees observed the insider's activities, but did not report anything unusual until it was discovered that a theft of proprietary information had occurred.

Importance of Communication within the Organization
An insider was very upset with a new supervisor, and resigned from the organization. Upon his resignation, the insider sent an angry letter to the human resources department outlining his complaints. Several days later the insider caused a disruption to the organization's systems. Human resources had not shared with anyone in the organization the level of anger and frustration communicated by the insider.

Behaviors of Concern
An insider had a history of poor work performance. He often could not be located in the building where he worked, and rarely worked the hours that he was assigned. The insider quit to take a new job and committed theft of intellectual property prior to leaving the company.

* * * * * * * * *

Coworkers noticed a sudden change in lifestyle with an insider who repeatedly refused to follow policies regarding password use. The insider was observed making luxurious purchases. It was discovered later that the insider had committed fraud.

* * * * * * * * *

An insider had a history of being difficult to manage at his place of employment. He would leave work in the middle of the day or work for several days at a stretch then disappear without notice. Coworkers stated that when the insider was on the job, they never knew if they would find the insider asleep in an empty office. The insider later quit and committed theft of intellectual property.

Advancing the Attack

Former System Administrator Uses Multiple Shared Accounts
A chief technology officer, who had full access to all system passwords, customer accounts, and confidential information for maintaining the company's network, resigned after a dispute over his salary. Less than a month later, he changed the company's voicemail system so that certain customers were directed to a pornographic telephone service. About a week later, he modified the company's email server so that anyone sending email to his old account received an automatic reply that disparaged the company and its services. A month and a half following his attack on the email server, the insider posted multiple threats on the company's website. Two and a half weeks later, the company president received an email sent from his own company email

account that said, “the world would be a better place without you,” and “say goodbye to anyone who pretends to care about you.”

Theft of Information Following Termination Because of Poor Password Practices
A former system administrator was able to log in following his termination using the password for the chief operating officer’s (COO) account. While employed as system administrator, he created default passwords for new accounts. The COO did not change his password; the insider consequently was able to use that password to log in following termination and download 340 sensitive company files.

Access Following Termination Due to Lack of Account Management
After 15 years of employment with a cable company, an insider was terminated from his position for behavioral problems. Although his employers disabled his account, they were unaware of a second account to which he had access. The insider used his company-owned laptop to access the company’s network remotely; tried his own account and, when that proved unsuccessful, used the second account to gain access. He then deleted data and software that the company used for daily operations. The impact of the attack was amplified by operational problems with system backups.

Theft of Information Following Termination Because Remote Access Was Not Disabled
An employee responsible for network security was terminated from his position, but his remote access was not disabled by his employer. Using that access, he downloaded and removed files from the network, deleted an event log, and made modifications to some files that were being worked on by his replacement.

Access Following Termination Using Unauthorized Backdoor Accounts
A system administrator set up his company’s servers so that he could access every computer remotely via telnet. When the insider’s employer notified him that they were considering laying him off since the systems were running so well, he became angry and created several fictitious accounts with full administrative rights. The day after he was fired, the insider accessed the systems remotely and reformatted all hard disks on all of the company’s computers, including all backup copies of the computer files stored on a backup server machine.

Fraud Facilitated When Employee Transfers But Retains Previous System Access Rights
When an employee transferred from her position in the payroll department to human resources (HR), she was given full access to the HR databases. Her access to the payroll system should have been disabled, but was overlooked. She subsequently executed a complex scheme based on her detailed knowledge of, and access to, both systems. For almost 10 months, she modified the HR database for terminated employees to falsely indicate their rehire at higher rates of pay; modified their home address in the payroll system to her own home address; and modified their direct deposit information to direct their pay to her husband’s checking account. When her fraud was detected, she had deposited approximately $198,000 into her husband’s account.

Insider Sabotages Entire Project Due to Lack of Fine-Grained Access Controls
A project manager for one component of a large project sabotaged the project by cutting wires, unplugging cables, connecting to the computer remotely and stopping compilations and builds of the code, and reformatting hard drives. In response to the insider's attack, the organization imposed limits on physical and electronic access so that team members could only access their portion of the project; the problems then stopped. The organization later loosened the access control restrictions, and the insider immediately resumed the malicious activity.

Vulnerability Posed by Default Passwords
One company implemented a standard algorithm for generation of passwords for new employee accounts; the password was set to the first letter of the employee's first name followed by the first seven letters of the last name. Employees were instructed to change the password upon first use, but no technical controls were imposed to enforce this policy. One insider, a supervisor, used this knowledge to commit fraud against his company using various computer accounts over a period of almost four years from which he derived approximately $500,000.

Detecting the Attack

Detection by Proactive Monitoring of After-Hours Network Activity
A temporary employee was hired as a customer service representative for the 3 p.m. to midnight shift. A system administrator noticed unusual network traffic occurring after midnight, and traced the activity to the insider's workstation. Upon investigating the nature of the suspicious file transfers, he found that at least one customer's VISA account number had been posted to the Internet. Additionally, other proprietary, copyrighted files had been copied and transferred over the Internet by the insider.

Detection by Creative Logging and Monitoring
An employee logged onto her computer and the automated login message indicated that her last login was one hour earlier. In fact, she had not logged into the system for several days. The shell history file showed that someone had logged into her computer and attempted to delete the shell history file so that evidence of the intrusion would be erased. The employee had renamed her history file, however, so that system activity was retained. An investigation showed that the intruder was a former contractor for the company who had been terminated for non-performance. He had been accessing the systems on a daily basis during working hours; up to 16 different computers and at least 24 different user accounts had been compromised. He read electronic mail, attempted to access his former supervisor's account, and reviewed source code for systems with trade secrets estimated to be worth approximately $1.3 million.

Concealing Identity
The office manager for the sales division of a computer software products distributor used a "remailer"[53] to send email to one of his company's competitors offering to sell them his company's customer database. The database contained names, addresses,

[53] A remailer is a computer service that facilitates sending email anonymously so that the sender cannot be traced or identified.

and contact information for all the company's current and potential customers as well as history of products purchased by each customer, expected future needs, and pricing information. The incident was detected when the competitor contacted his company. Law enforcement was able to trace the email to the insider's computer because the remailer substituted a proxy email account for the sender, but the IP address of the sender was unchanged.

Importance of Preserving System Logs

Multiple employees of a subcontractor for a large telecommunications company defrauded the parent company for $500,000 over a period of almost four years. All changes to individual database records were tracked inside the telecommunications company's database; investigation showed fraudulent activity had been taking place for almost four years. However, system logs of account logins were recycled monthly; specific activity by login account and computer used was only available for one month. Since the insiders used shared training accounts to make the changes to the database, the logins to those accounts could only be traced back to the originating personal computer accounts for one month of activity.

Consequences to the Organization

Harm to Company's Reputation

After serving as a consultant for a company for one year and an employee of that company for one month, an insider was fired when he was found by his employer to have concealed a prior criminal history. During his employment, this insider had copied the company directory; the board member home telephone and address list; and confidential salary information. After his termination, he posted numerous threats against various people connected with the company and a large number of social security numbers to a web site.

Successful Prosecution Due to Signed Intellectual Property Agreement

The insider was hired as a product support engineer for a small startup company's computer security product. The following month his company was acquired by a large IT company, and he went to work there after signing the company's standard intellectual property agreement. That same month, he approached a few people about starting a competing company, and approximately four months later the insider and his colleagues began coding the new product. The insider continued to work at the IT firm and worked on his competing product in his spare time over a period of eight months. At that time, he resigned his position, taking with him a backup tape containing the software for the two most recent releases of the product. Approximately nine months later, he announced the first release of his new product. He was successfully prosecuted as a result of the agreement he signed upon employment with the IT firm.

Successful Theft of Intellectual Property Due to Lack of Signed Agreements

An independent contractor was hired to develop software, but no signed contract gave the hiring company ownership of the software. Six months after the insider quit working for the company, he still retained access through the firewall from his home computer, and his account was not disabled. The insider, along with a second former contractor, opened FTP and telnet sessions to the company's computer and copied the source code for the product they had been working on, including software they wrote as well as software written by others. They then proceeded to sue the company for using software that belonged to them, and the company sued them for stealing software that belonged to the company. Due to the lack of a contract, as well as the fact that the company was attempting to obtain venture capital at the time, the company chose to pay each of the contractors $30,000 to drop the charges.

APPENDIX D: Glossary of Technical Terms[54]

access controls: the rules and mechanisms that control access to information systems and physical access to premises.

account audit: process of verifying that all system computer accounts are valid, that is, that they are assigned to a valid user, that the user is aware of the account's existence, and that the user still has a legitimate need for that account.

authorized access: explicit permission to use.

autonomous agent: a self-contained program that is capable of making independent decisions and taking actions to satisfy internal goals based upon its perceived environment.[55]

backdoors: in computer and network systems, unauthorized means for gaining access to the system known only to the person who installed them.

business rule check: method for comparing data to a definition reflected in the design of a database for checking data integrity and flagging inconsistencies.

critical assets: an organizational entity essential to the organization's mission or efficient functioning.

coding: composing sequences of instructions for execution on a computing system (also known as programming).

configuration management: procedures or software for tracking releases and changes to software components so that previous versions can be recreated. It can also prevent unauthorized access to files or alert appropriate users when a file has been modified or released. Hardware configuration management can be facilitated through maintenance of a database containing information about the workstations, servers, bridges, routers, and other equipment on the network.

Database Administrator (DBA): the person responsible for the architecture, configuration, operation, security, maintenance, performance, and/or backup/recovery of a database.

DBA account: a privileged account that is used to perform Database Administrator functions.

[54] Many of these definitions are taken from the Information Security Glossary (http://www.yourwindow.to/information-security/)

[55] http://en.wikipedia.org/wiki/Autonomous_agent

denial-of-service attack: an attack directed towards a service, computer system, or network with the objective of making it inaccessible to legitimate users.

DNS server (Domain Name Service): an Internet service that translates domain names (like www.cert.org) into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet, however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.[56]

domain name: unique name that identifies an Internet site, for example, www.secretservice.gov.

fine-grain access controls: describe rules and mechanisms that apply at the individual file level or below.

flooding: a user accesses a target repeatedly in order to overload the target's capacity.

FTP (File Transfer Protocol): a protocol and command used to transfer files from one computer to another.

information exchanges: a means of obtaining information either from other attackers (such as through an electronic bulletin board), or from the people being attacked (commonly called social engineering).

IP address (Internet Protocol address): number used to uniquely identify computers on the Internet.

logic bomb: malicious code implanted on a target system and configured to execute after a designated period of time or on the occurrence of a specified system action.

privileged users: users who have an elevated level of access to a network, computer system, or application. For example, system administrators, network administrators, and Database Administrators (DBAs) have the ability to create new user accounts and control the access rights of users within their domain.

probing: accessing a target in order to determine its characteristics and/or vulnerabilities.

rogue accounts: accounts that exist without authorization.

root access: system administrator access on Unix-based operating systems.

scanning: attempts to learn about the weaknesses of a computer or network by repeatedly sending it requests for information.

[56] This definition was taken from www.surpac.com/refman/default/ssilm/glossary.htm

spoofing: impersonating another person or computer, usually by providing a false email name, URL, or IP address.[57]

telnet: a program and protocol that allows one to connect to another computer on a network. After providing a username and password to login to the remote computer, one can enter commands that will be executed as if entered directly from the remote computer's console.[58]

toolkit: a software package often distributed on hacker websites containing a variety of malicious or obfuscating programs.

trusted baseline: a state of a computer system which is known or assumed not to contain malicious content or programs.

two-person control: the close surveillance and control of a system, process, or materials at all times by a minimum of two authorized persons, each capable of detecting incorrect and unauthorized procedures with respect to the tasks to be performed and each familiar with established security requirements.[59]

Virtual Private Network (VPN): encrypted sequence of communication often used to provide secure remote access to an organization's network via the Internet.

[57] This definition was taken from www.keybank.com/html/A-11.2.1.html

[58] This definition was taken from www.orafaq.com/glossary/faqglost.htm

[59] This definition was taken from R.W. Shirley, “Internet Security Glossary.” The Internet Society/Internet Engineering Task Force RFC 2828, May 2000.

APPENDIX E: Acknowledgements

The Secret Service and CERT appreciate the work and dedication of the following personnel, without whose efforts this study would not have been possible. With many thanks to the ITS staff:

U.S. Secret Service, National Threat Assessment Center
Brandi Justice
Diana McCauley
Eileen Kowalski
Georgeann Rooney
Jim McKinney
Karen Damato
Lea Bauer
Lisa Eckl
Marisa Reddy Randazzo, Ph.D.
Megan Williams
Michelle Keeney, Ph.D.
Susan Keverline, Ph.D.
Tara Conway

Carnegie Mellon University, Software Engineering Institute, CERT Program
Andy Moore
Bill Wilson
Bradford Willke
Casey Dunlevy
Chris Bateman
David Mundie
Dawn Cappelli
Mark Zajicek
Stephanie Rogers
Tim Shimeall
Tom Longstaff

Also, the Secret Service and CERT gratefully acknowledge the contributions of: former NTAC Research Coordinator, Dr. Marisa Reddy Randazzo, who founded and directed the study within NTAC; former NTAC Special Agent In Charge, Matt Doherty, whose persistent outreach efforts furthered the study’s completion; Gwen A. Holden whose insights and skillful editing helped to shape the ITS reports; Dr. Eric Shaw whose valuable observations resulted in improved content; and, Special Agents Cornelius Tate, Dave Iacovetti, and Wayne Peterson for their consistent liaison efforts.